日立グループの総合力を結集したトータルソリューションをご提案します。

ポリシーの策定からシステム構築および運用･監視、監査、物理セキュリティにいたるまで、セキュリティに関するさまざまなニーズに対応。日立グループのセンターによる運用･監視サービスや全国拠点からのオンサイトサービスなど、総合力のある日立ならではのワンストップサービスを提供します。

各社問い合わせ先

- ●株式会社 日立アドバンストシステムズ www.hitachi-as.co.jp/
- ●株式会社 日立インフォメーションアカデミー www.hitachi-ia.co.jp/
- ●株式会社 日立公共システム www.hitachi-gp.co.jp/
- ●株式会社 日立産業制御ソリューションズ www.hitachi-ics.co.jp/
- ●株式会社 日立システムズ www.hitachi-systems.com/
- ●株式会社 日立システムズパワーサービス www.hitachi-systems-ps.co.jp/
- ●株式会社 日立情報通信エンジニアリング www.hitachi-ite.co.jp/
- ●株式会社 日立セキュリティサービス www.hitachi-ss.co.jp/
- ●株式会社 日立ソリューションズ www.hitachi-solutions.co.jp/
- ●株式会社 日立ソリューションズ･クリエイト www.hitachi-solutions-create.co.jp/
- ●株式会社 日立ハイテクソリューションズ www.hitachi-hightech.com/hsl/
- ●株式会社 日立保険サービス www.hitachi-hoken.co.jp/
- ●株式会社 ニッセイコム www.nisseicom.co.jp/
- ●株式会社 エー･シー･エス www.acs21.co.jp/
- ●株式会社 日立製作所 www.hitachi.co.jp/

セキュリティ統制

- セキュリティポリシー
- 法令遵守
- セキュリティ運用
- ログ証跡管理
- 診断／監査

ID管理	・統合ID管理	・特権ID管理
物理セキュリティ	・入退管理 ・物品管理	・施設管理
データセキュリティ	・情報保護 ・アクセス制御	・暗号化 ・改ざん検知
ネットワークセキュリティ	・接続端末認証 ・サイバー攻撃対策	・不正アクセス監視 ・マルウェア対策

安全に関するご注意　正しく安全にお使いいただくため、ご使用の前に必ず「取扱説明書」、「使用上のご注意」などをよくお読みのうえ、おまもりください。

● カタログに記載の仕様は、製品の改良などのため予告なく変更することがあります。● 製品の色は印刷されたものですので、実際の製品の色調と異なる場合があります。
● 本製品を輸出される場合には、外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。
なお、ご不明な場合は、弊社担当営業にお問い合わせください。

製品に関する詳細･お問い合わせは下記へ

■ 製品情報サイト
http://www.hitachi.co.jp/secureplaza/

■ インターネットでのお問い合わせ
http://www.hitachi.co.jp/secureplaza-inq/

株式会社 日立製作所　情報･通信システム社　クラウドサービス事業部

SP-704-30 | 2015.5
Printed in Japan(B)

日立セキュリティソリューション「Secureplaza」ソリューションパック2015

HITACHI
Inspire the Next

安心を積み重ねることで、
明日のビジネスが見えてくる。

セキュアプラザ
Secureplaza

リスク管理に基づいたセキュリティ戦略が、企業経営の基盤に。

事業継続のためのセキュリティは、企業の社会的責任です。

あらゆるビジネス活動や人々の暮らしがIoTの進展に伴いつながる時代。
ひとたび企業の情報システムが止まれば、その損害は自社のみにとどまらず、
顧客や株主、サプライチェーン全体へとおよびます。
ITシステムのセキュリティは、ビジネス活動を支える要となっており、
セキュリティの確保は、今や事業継続の観点から企業の社会的責任となっています。

さまざまなリスクへの対処、CSR(企業の社会的責任)への対応

1 ITを取り巻く脅威への対応
- サイバー攻撃
- 内部不正
- 自然災害
- ハクティビズム

2 コンプライアンス 内部統制
- 個人情報保護法
- 不正アクセス禁止法
- サイバーセキュリティ基本法
- 金融商品取引法（日本版SOX法）

3 国家施策 標準化・ガイドライン
- ISO/IEC 27001、15408
- マイナンバー制度
- 政府機関統一基準
- 業界ガイドライン
- PCI DSS

→ **企業価値の向上 企業ブランドの向上 安全な社会インフラ**

目的に沿ったソリューションによりあらゆる情報リスクをカバーします。

日々変化する脅威やさまざまな法令・ガイドラインについて、最新情報を常に入手し、
それらへ網羅的に対応することは容易なことではありません。
日立のセキュリティソリューション「Secureplaza」では、脅威・課題に応じた目的別ソリューションにより、
次の3つの側面から多様なITシステムのリスクをトータルにカバーします。

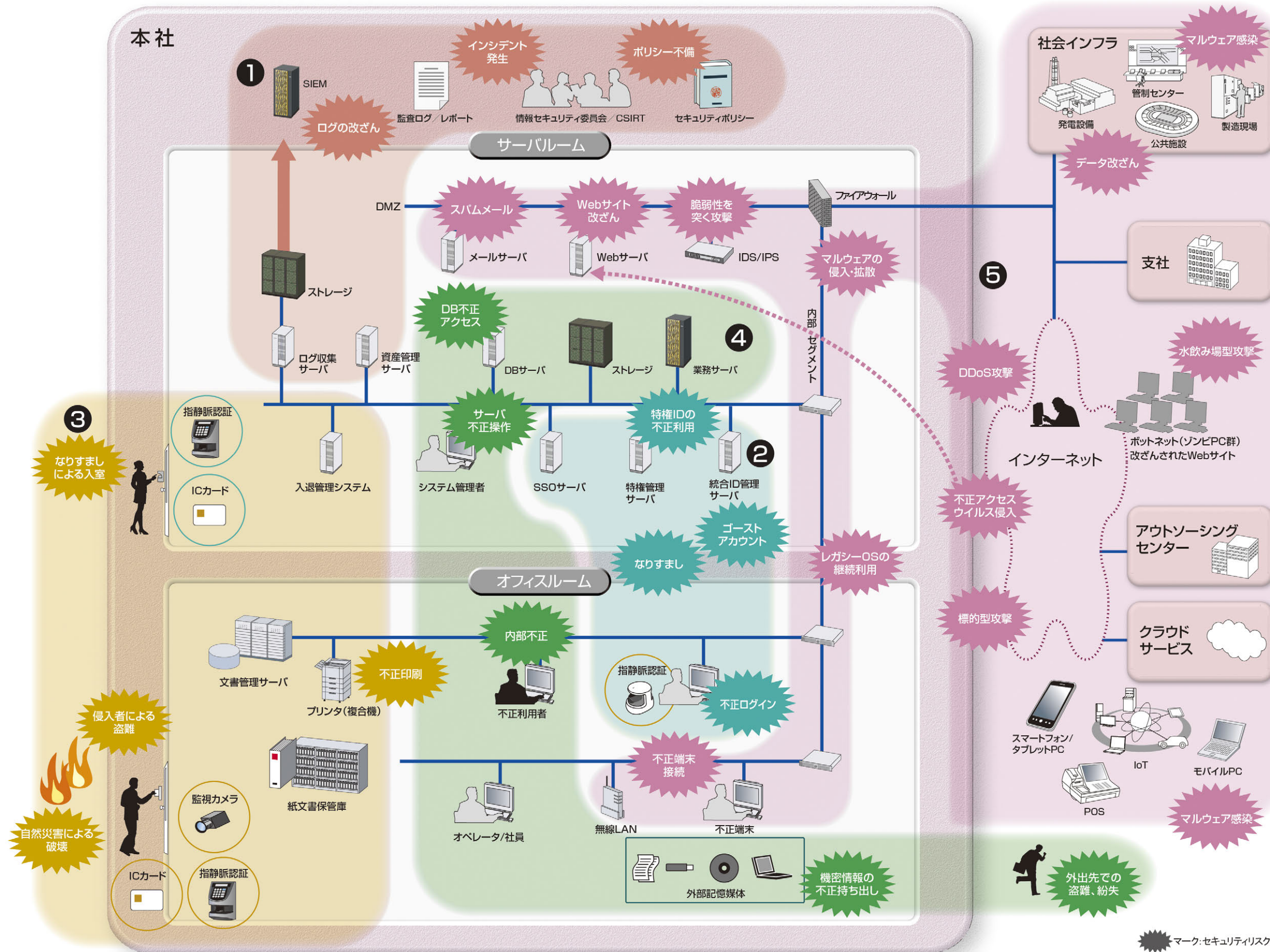
1. ITシステムを取り巻く脅威に対する対策
2. コンプライアンス・内部統制の観点
3. 国家施策や各種標準化・ガイドラインへの対応

お客さまの経営戦略に即した情報セキュリティを確立するだけでなく、
対策レベルに応じた実現策の見直しを可能とすることで、継続的な改善を実現します。
さらに、お客さまの事業継続と企業価値の向上に加え、
より安全な社会インフラの実現をセキュリティ面からサポートします。

IoT:Internet of Things 家電や自動車など、あらゆるモノがインターネットに接続されること
ハクティビズム:社会的・政治的な主張のもとに、ハッキング活動を行うこと
PCI DSS : Payment Card Industry Data Security Standard

ソリューションカテゴリ	脅威・課題	Secureplaza対応ソリューション
セキュリティ統制	セキュリティ規則・ルールの不備 内部不正・証跡不備 インシデント対応	1 組織内のセキュリティガバナンスと維持 Secureplaza/GR Governance and Risk Management
ID管理	なりすまし 業務システムのアカウント管理 特権IDの不正利用	2 利用者・端末の正当性を確保 Secureplaza/IM Identity Management
物理セキュリティ	施設への不正侵入 書類・物品の盗難・紛失・誤廃棄 設備・物品のライフサイクル管理	3 物理的な侵入行為からの防御 Secureplaza/TZ Trusted Zone Management
データセキュリティ	データの盗難・紛失 データの破壊・改ざん データの二次流出	4 情報資産の保護と適切な資産利用の促進 Secureplaza/DS Data Securty
ネットワークセキュリティ	マルウェア感染・脆弱性を突く攻撃 インターネットからの不正アクセス 公開Webサイトへの攻撃	5 ネットワーク上の脅威からの保護 Secureplaza/NS Network Security

オフィスのあらゆる情報リスクを、全方位からカバーするトータルソリューション。

企業の情報資産の実態を明らかにし、リスクレベルに応じた対策を提案するコンサルティングサービスから、最新技術を 駆使したシステム構築、運用管理まで一括したサービスを提供します。
高度情報化されたITシステムや社会インフラに対する被害を未然に検知・防御します。

❶ 組織内のセキュリティガバナンスと維持
Secureplaza/GR
Governance and Risk Management

エンタープライズリスクマネジメントに不可欠な、セキュリティポリシーの策定やCSIRT体制の確立、SIEMによるSOC構築を実現します。

❷ 利用者・端末の正当性を確保
Secureplaza/IM
Identity Management

より確実な本人認証や、組織システム利用者管理の効率化、特権ユーザー管理などで、ID管理を実現します。

❸ 物理的な侵入行為からの防御
Secureplaza/TZ
Trusted Zone Management

セキュリティレベルに応じたゾーニングに基づく入退管理や、書類・機器など物理資産の効率的かつ安全な管理を実現します。

❹ 情報資産の保護と適切な資産利用の促進
Secureplaza/DS
Data Security

組織内での不正行為や、外出先での盗難・紛失など、さまざまな脅威から組織の情報資産を保護します。

❺ ネットワーク上の脅威からの保護
Secureplaza/NS
Network Security

サイバー攻撃など、ネットワークを介した脅威から組織ネットワークを保護します。また、リモート接続など、さまざまな利用形態に即したセキュリティ施策を実現します。

SIEM :Security Information and Event Management
CSIRT :Computer Security Incident Response Team
DMZ :DeMilitarized Zone
IDS :Intrusion Detection System
IPS :Intrusion Prevention System
SSO :Single Sign-On
DDoS :Distributed Denial of Service
SOC :Security Operation Center
IoT :Internet of Things 家電や自動車など、あらゆるモノがインターネットに接続されること
POS :Point of Sale
ボットネット：サイバー犯罪者が乗っ取った多数のゾンビPCから構成されるネットワーク
ゾンビPC：サイバー犯罪者が不正プログラムなどを使用して乗っ取ったPC

組織のセキュリティ維持に欠かせないポリシーの策定や セキュリティインシデントへの対応体制をシステム、運用の両面から確立し、継続的な セキュリティレベルの維持を支援します。

インシデントの的確な把握と迅速な対応を、基盤・運用システムの両面から支援します。

- 報道などで発生しているセキュリティ情報への対応状況を知りたい
- 投資を抑えつつ効率的なセキュリティ施策を行いたい

- 証跡を取得しているが、アラートが多すぎてどこから対応してよいか分からない
- 至急対策をしなければいけないが、何をすればよいか分からない

組織のセキュリティ施策の基礎となるポリシーの制定

・ポリシー策定/監査　・セキュリティアセスメント

組織の活動を支える情報インフラの健全性を確保

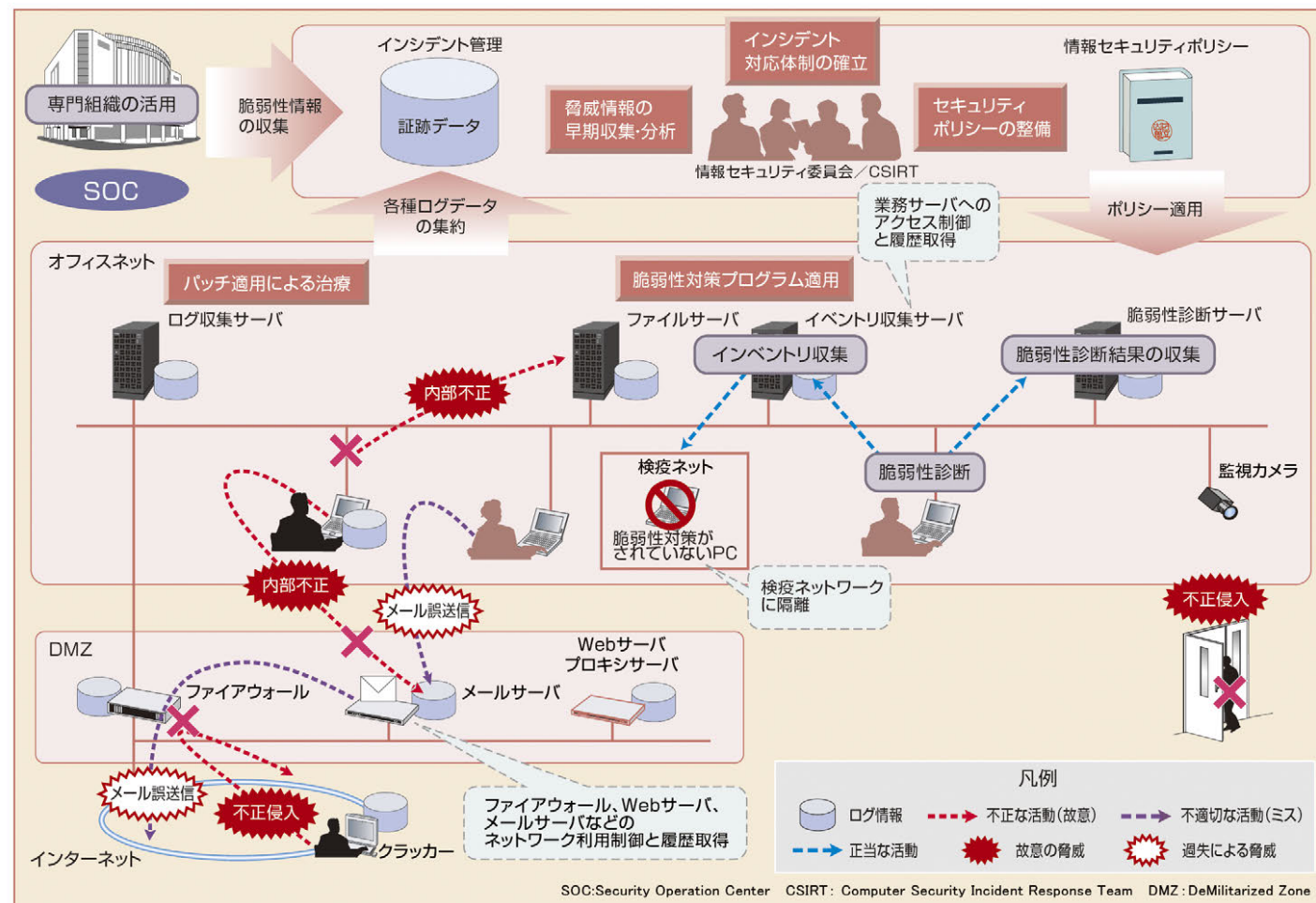
・脆弱性対策　・ログ管理

インシデント発生時の適切な対応

・インシデント対応体制整備　・専門組織との外部連携

脆弱性情報の管理とログの収集により、組織インフラの健全性を確保します。

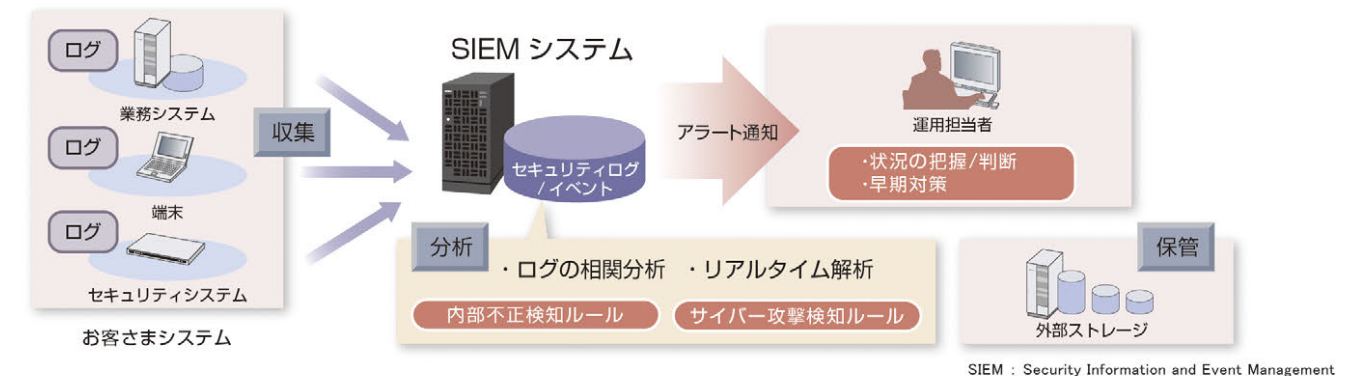
組織インフラの脆弱性情報の収集から修正までの総合的な脆弱性対策を提供します。また、さまざまな場所で発生するログデータを取得・分析・保管することで、インシデント発生時に必要となるタイムリーな対策や証拠性の確保などをトータルに実現します。さらにセキュリティ専門要員による運用監視を提供することで、より高度な組織インフラの維持を実現します。

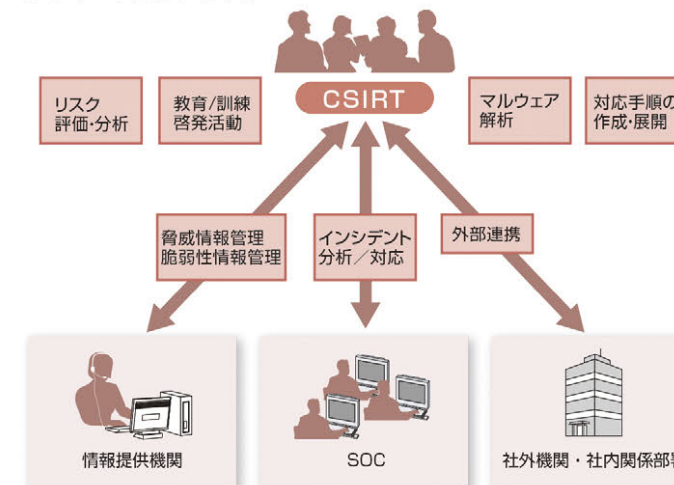
SOC:Security Operation Center　CSIRT：Computer Security Incident Response Team　DMZ：DeMilitarized Zone

セキュリティガバナンスを維持するうえでは、「収集・保管」「分析・対策」「監査」の3つの側面から網羅的な対応が必要です。

分類		具体的対応		
収集・保管	組織内	ログイン履歴 メールフィルタリング履歴 Webアクセス履歴 マルウェア検出の履歴 外部記憶媒体への出力履歴	ファイルアクセス履歴 メールアーカイブ DBアクセス履歴 印刷履歴	特権ユーザー操作履歴 認証強化(ICカード、指静脈)による取得ログの真正性向上 パケットキャプチャ 統合ログ管理
	組織外との境界	入退記録(ログ・映像など) ネットワーク(FW、IDS/IPS、Proxy、無線LANなど)通信の記録		
分析・対策	分析	人手による単体分析	リアルタイム分析	複数ログの相関分析
		インシデント原因分析	監査ツールによる分析	専門家のインシデント調査
	アクション	接続ポート閉塞	ネットワーク接続の遮断	監視ルールのアップデート
監査	監査	人手による不正チェック	監査ツールによる不正チェック	外部監査の受査

IDS：Intrusion Detection System　IPS：Intrusion Prevention System

サイバー攻撃や内部不正の予兆の早期発見にはセキュリティログやイベントログの収集・分析が効果的です。

SIEM：Security Information and Event Management

CSIRT構築運用支援ソリューション

セキュリティインシデントの発生から解決、再発防止までを組織横断で対応するCSIRT構築、運用をサポートします。
また、SOC構築や組織外連携によりインシデントの予兆を収集し事前対応へのサポートを行います。

コンサルテーションサービスメニュー

情報セキュリティマネジメントコンサルテーション

- 情報セキュリティポリシー策定コンサルティング
- IT全般統制コンサルティング
- ISO／IEC27001認証取得コンサルティング
- ISO／IEC20000認証取得コンサルティング
- プライバシーマーク認定取得コンサルティング
- 個人情報保護法対策コンサルティング
- 事業継続マネジメント策定コンサルティング
- CSIRT構築支援コンサルティング
- CSIRT運用支援サービス

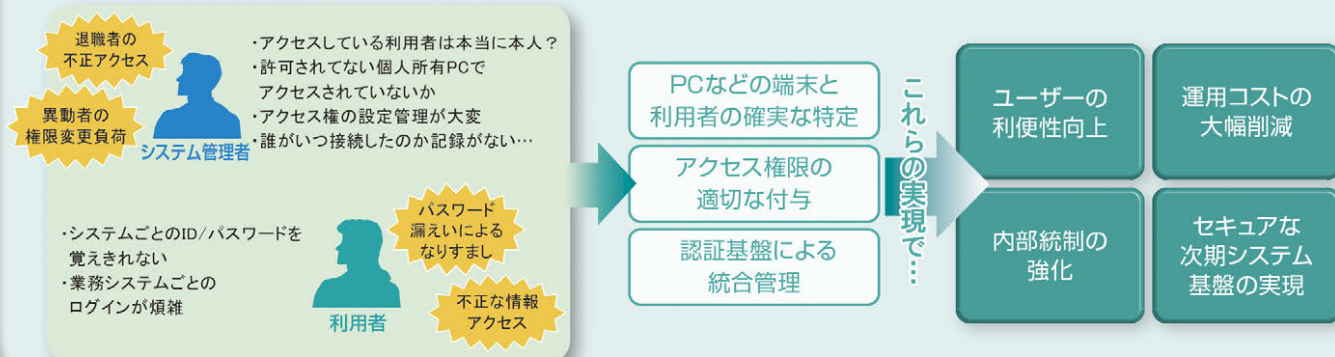
セキュアシステム設計・構築コンサルテーション

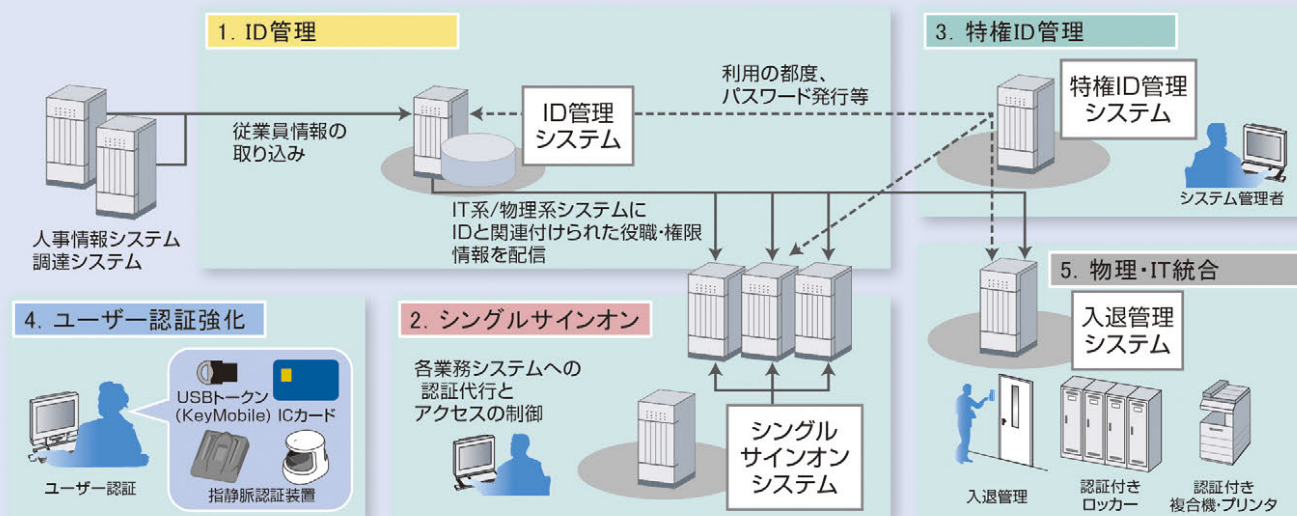
- 情報セキュリティシステム設計コンサルティング
- PCI DSS対応コンサルティング

情報セキュリティ診断・監査・教育サービス

- セキュリティアセスメントサービス
- セキュリティホール診断サービス
- Webアプリケーション診断サービス
- ソースコード診断サービス
- 標的型攻撃対策状況診断サービス
- 情報セキュリティ監査サービス
- セキュリティ教育支援サービス
- CSIRT要員育成サービス

PCI DSS：Payment Card Industry Data Security Standard

「アイデンティティ･マネジメント」は、さまざまなセキュリティ対 策の出発点。組織が実施すべきセキュリティ対策の実行基盤を確立します。

企業におけるアイデンティティ管理基盤の整備をトータルで支援します。

利用者の認証強化（PKI、指静脈認証など）、利用者情報の一元管理、シングルサインオンによる利用者の利便性向上など、ID管理に関わるソリューションを、トータルかつワンストップで提供。オープン化、仮想環境利用などにあたり、次期システム基盤のセキュリティ強化の基礎となる特権ID管理を効果的かつ効率的に実現します。

PKI : Public Key Infrastructure

アクセスコントロールの4つの要素（認証･認可･管理･監査証跡）で利用者のアイデンティティ情報（ID）とシステムリソース、権限を正しく対応づけ、その対応を維持しつづける仕組みが必要です。

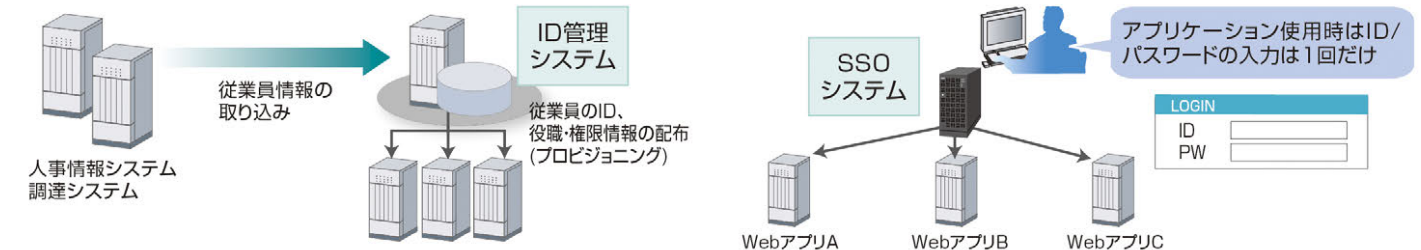
要素	機能	説明
認証：Authentication 本人認証/端末認証	･本人（利用者）認証	指静脈認証やICカードなどを利用した二要素認証により利用者を認証します。
	･端末認証	デバイス固有情報、デバイス証明書を利用した確実な端末認証手段を提供します。確実な端末認証により許可された端末のみ企業ネットワークへの接続を許可します。
認可：Authorization アクセス制御･管理	･ワークフロー	社内システム利用者IDの不正登録を防止するため、ワークフローによるID登録･変更･削除申請を実施します。
	･プロビジョニング	源泉となる人事情報の所属情報･属性を元に、対象となる社内システム、および社内物理系システムに対しIDの自動配信を行います。
	･シングルサインオン	シングルサインオン（SSO）により、利用者は一度の認証だけで、許可されたすべてのシステムへのアクセスが可能になります。
管理：Administration 運用管理/プラットフォーム管理	･ポリシー管理	ID単位のライフサイクル（登録/変更/失効）を、関連するすべての業務システムへのプロビジョニングルールに設定します（ロールベース/ルールベース）。
	･パスワード管理	パスワードポリシーに基づいた、ユーザーのパスワード変更を促します。また、パスワード管理におけるヘルプデスクや対象システムへのパスワード変更結果を自動配信します。
	･特権ID管理	特権IDの発行･管理、利用期間制御、アクセス制御の実施により、管理者による不正（情報漏えい、ログの改ざん、など）を防止します。
監査証跡：Auditing 不正抑止/証跡管理	･権限分離	企業に散在する業務システムに対して、統合的なユーザー管理･アクセス制御を行うことにより、ユーザーの権限分離を徹底･監査することができます。
	･ログ収集	システムへのアクセスログなどを収集し、監査証跡として活用できます。

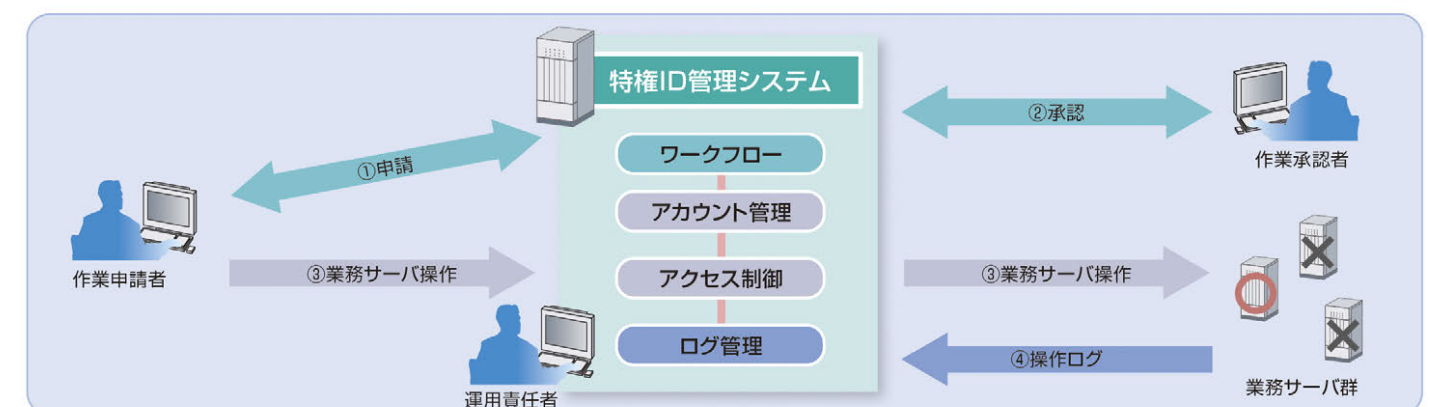
SSO : Single Sign-On

1. ID管理

ID利用者の異動、退職、権限変更時に、各業務システムへのID権限変更管理が一元的に行えます。ID管理作業（アクセス権設定や棚卸し）の効率化、監査対応の効率化を実現します。

2. シングルサインオン

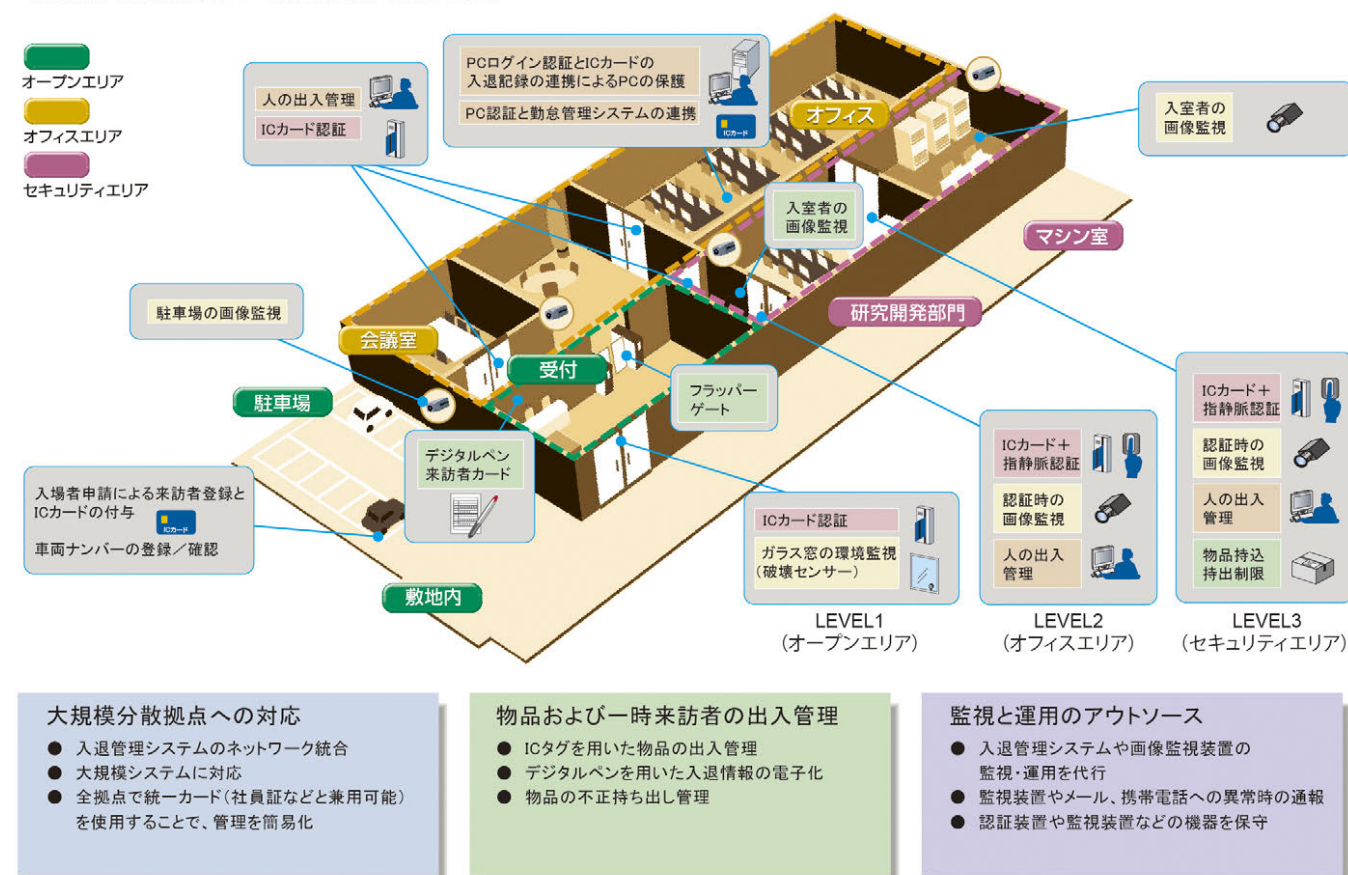
業務アプリケーションに“自動ログイン”し、業務アプリケーションへのアクセススピードが“画期的に向上”します。

3. 特権ID管理

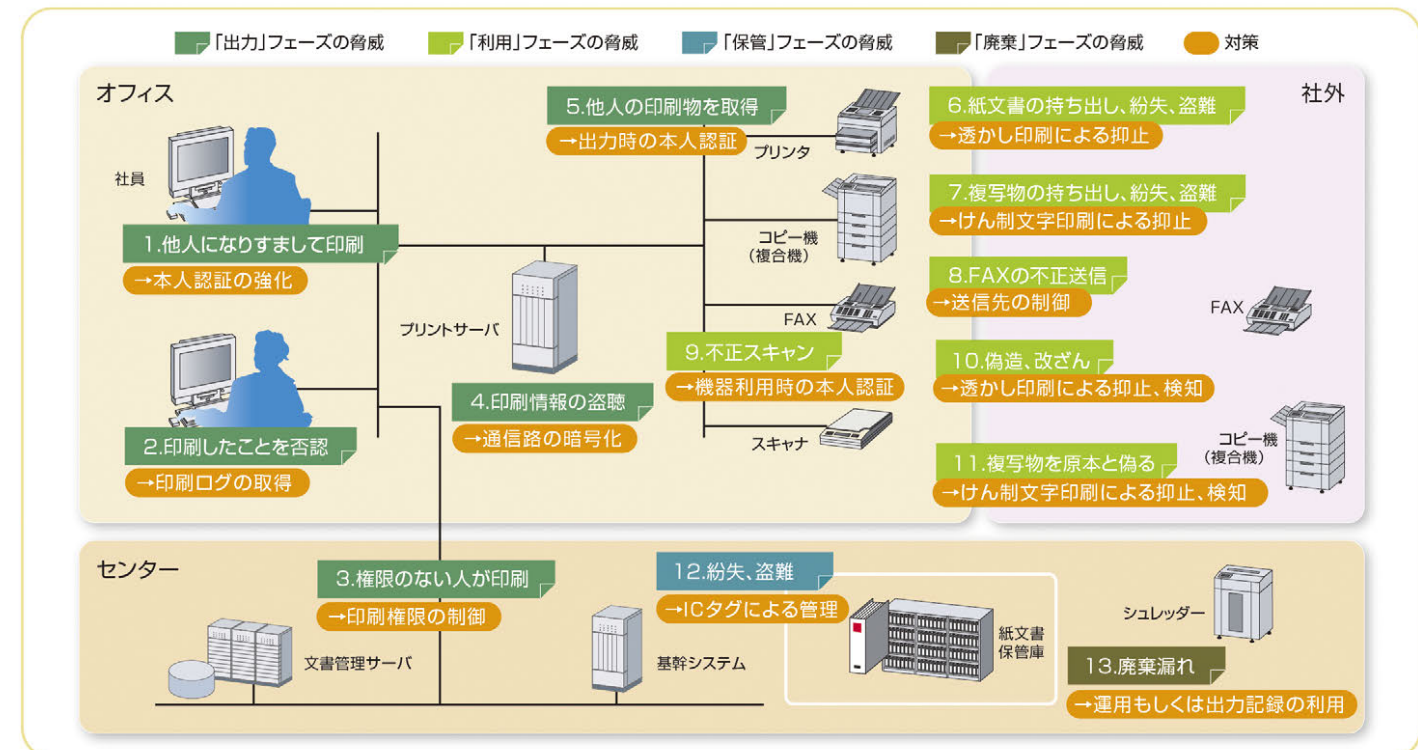
特権ID管理の不備による監査指摘や内部不正のリスクを低減します。

セキュリティレベルに応じたゾーニングによる入退室管理 や 書類・機器など物理資産の効率的かつ安全な管理を実 現します。

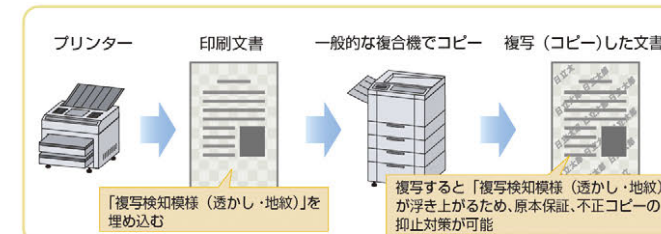
物理とITとの連携により高度な物理セキュリティを実現します。

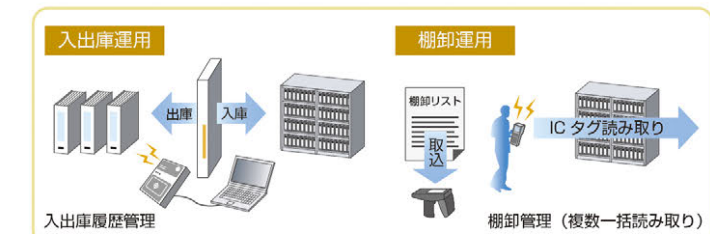
入退管理や物品管理を軸に、物理とITのセキュリティ連携を実現します。

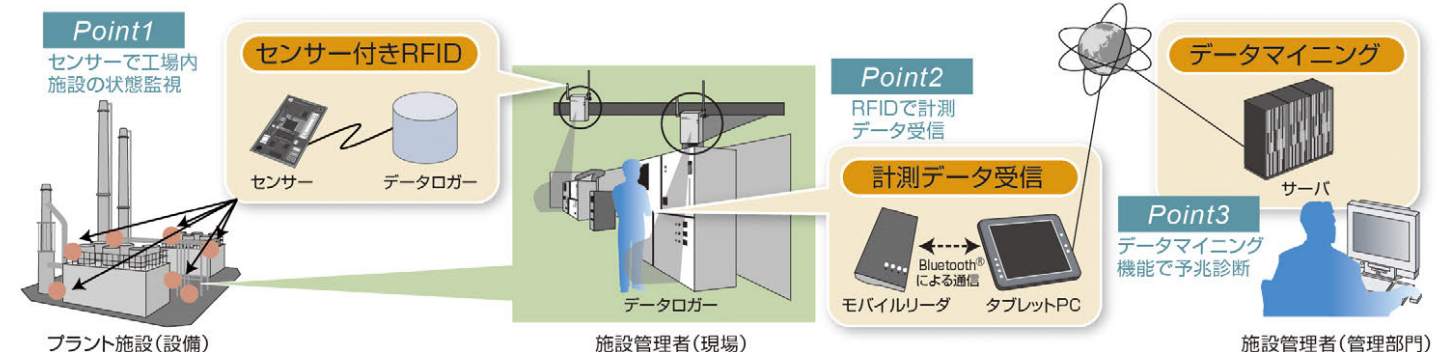
管理対象	監視内容	対策例
① 人	・不審者・第三者の侵入を許さない。 ・入退記録の無い者のシステムログインを許さない。	入退管理 ・ICカード認証 ・カメラ監視
② 物	・管理されている物を持ち出させない。 ・業務に関係のない物を持ち込ませない。	物品管理 ・所在/棚卸管理 ・出庫管理

エリアの重要度に応じて段階的なアクセス制御と監視を行い、施設への物理的な侵入行為を防ぎます。

セキュリティを考慮した紙文書のライフサイクル管理を実現します。

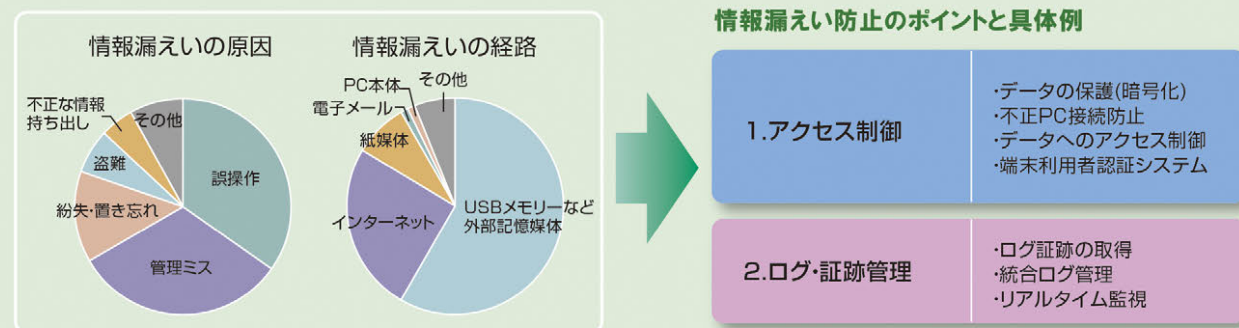
紙文書の出力・利用・保管・破棄の各フェーズで想定される脅威に対して適切なセキュリティ施策を実施します。

不正コピーの抑止対策

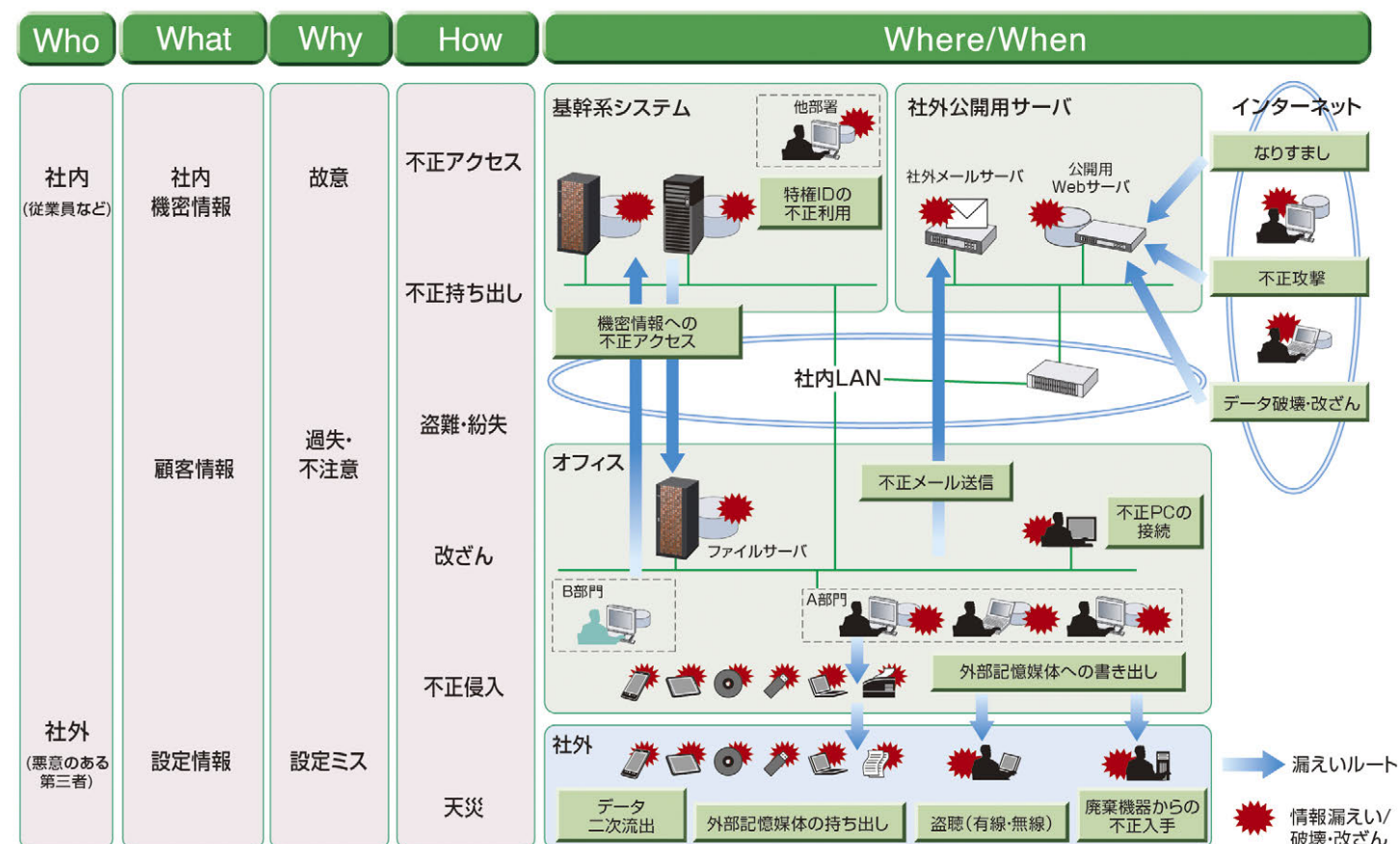
埋め込みにより不正コピーの抑止対策を実現します。

重要文書管理

ICタグを重要文書に貼り付け、各種リーダで読み取り、重要文書を管理します。

プラント施設（設備）やパイプラインなどの老朽化による被害を未然に予測します。

RFID技術により、人の立ち入りが危険な環境にあるセンサー情報を安全な場所から収集・分析します。
膨大なデータ解析を、データマイニングサービスで解析し、事故の予兆を未然に解析します。

さまざまな脅威から組織の情報資産を保護し、適切な制御をすることで、安全な情報資産の利用を実現します。

情報の漏えいや侵害のリスクは、日々の業務に潜んでいます。

情報の漏えいや侵害(破壊・改ざんなど)の原因・経路は、多岐にわたります。
情報漏えいの防止には業務全体を俯瞰し優先度を決め、「アクセス制御」「ログ・証跡管理」の観点から対策アプローチを検討することが重要です。

5W1Hで、あらゆる業務形態、漏えいルートを調査・分析します。

「いつ」「どこで」「誰が」「何の目的で」「どうやって」「何の情報が」漏えいするか、侵害されるかをトータルに診断・分析。
情報管理形態や日々の業務を考慮した効果的なツールの導入により、セキュアな業務を実現します。

脅威の内容に応じた、さまざまなデータセキュリティを提供します。

日々の業務に潜む脅威や組織の運営に付随する脅威に対し、適切な対策を実現する手段を複数提供します。また、それらの多様な対策を効果的・効率的に実施していくために必要な「現状分析」「対策計画策定」「システム構築」「運用・監査」を総合的に支援します。

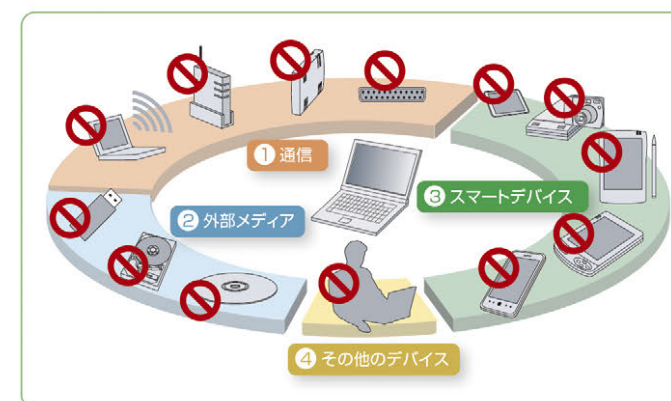
脅威	対策		Level 1	Level 2	Level 3
内部不正	監査	監査	人手による監査レポート作成	監査ツールによる不正チェック	外部監査の受査
不正アクセス	監視・分析・アクション		定期的なログ分析	ルールベースのログ分析	シナリオベースのログ分析
訴訟・事故	ログの収集・保管		機密情報へのアクセスログ取得	全てのログデータの取得	統合ログ管理
データ二次流出	データ利用権管理	制御・抑止	秘密保持契約の締結	IRMによるデータ保護	DRMによる所有者管理
PC・スマートフォン盗難紛失	データ暗号化・秘匿		PC、スマートデバイスの資産管理	紛失時のデータ保護(リモートワイプなど)	端末へのデータ保管禁止(端末のシンクライアント化)
データの盗難・紛失	データ保護		データ自体の暗号化	データへのアクセス制限	RFIDなどによる持ち出し管理
データ破壊・改ざん	データ管理		データへのアクセス制限	データのバックアップ・ディザスタリカバリ	データの改ざん検知
不正アプリ導入などによる情報漏えい	資産管理		インストールアプリの情報収集	ライセンス管理・モバイルデバイス管理	アプリケーションのインストール制限
データ持ち出し ※ネットワーク経由	暗号化・フィルタリング		メール/Webフィルタリング	暗号化メールの利用	データ中心型情報漏えい防止対策
データ持ち出し ※外部記憶媒体	持ち出し/アクセス制御		外部記憶媒体の利用制限	データ保管領域へのアクセス制限	承認ベースの持ち出し制御
特権IDの不正利用	特権管理	認証	承認による特権ID発行	役割ベースの特権IDアクセス制御	特権IDの強制アクセス制御
なりすまし	認証(人・機器)		デバイス認証(ICカードなど)	接続端末認証	本人認証(指静脈認証など)

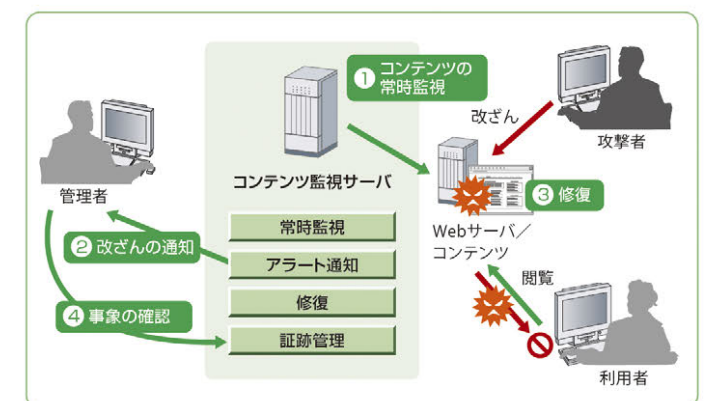
データ保護の基盤

セキュリティガバナンスの適用 – セキュリティポリシー、ベースラインなど –	ID管理基盤の構築 – アカウント取り扱いルール、統合ID管理、など–	物理的な不正侵入行為からの防御 — 入退室管理、カメラ監視、など –

IRM : Information Rights Management　DRM : Digital Rights Management　RFID : Radio Frequency IDentification

デバイス制御による持ち出し対策

PCに接続できるスマートフォンやUSBメモリーなどの利用をコントロールすることで、情報漏えいのリスクを低減します。

Webコンテンツ改ざん検知・修復対策

Webサイトの改ざんを早期に検知・修復します。
企業ブランドの損失を未然に防ぐと共に、水飲み場型攻撃へ悪用されることを防ぎます。

組織内外での不正アクセスをネットワークレイヤで防御。インシデントの未然防止、および被害を最小化するネットワークを実現します。

急増するネットワーク上の脅威

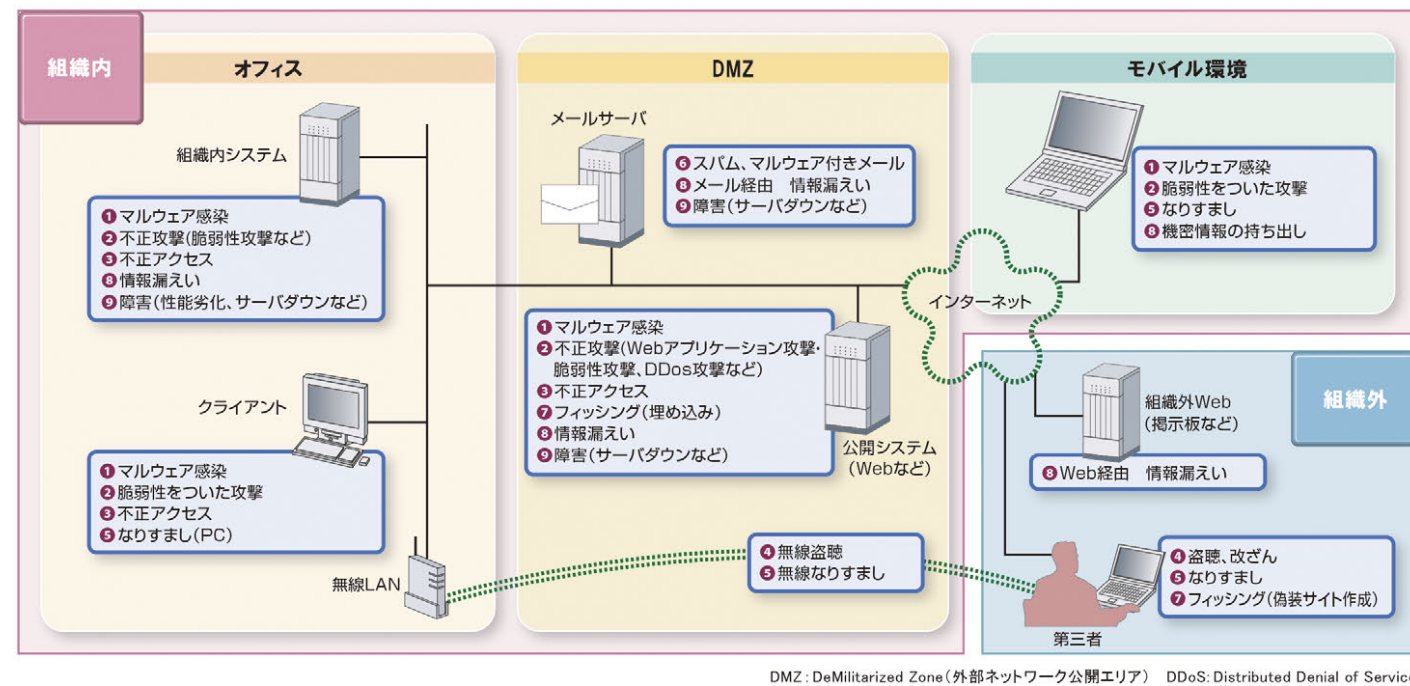
ネットワークを介した脅威は、年々増加しています。メールやWeb、モバイルからなど経路は多様化し、攻撃の手口もフィッシングや特定の企業や個人を狙う「標的型攻撃」という方向へ、より巧妙化しています。

・不正アクセス件数が過去最高に…
・Webアプリケーションに対する攻撃が急増…
・受信メールのほとんどがスパムだ…
・フィッシング被害が急増している…

ネットワークセキュリティ設計方針と施策の検討ポイント

- ネットワークセグメントのゾーニング
- 各セグメント間通信のアクセス制御
- ネットワーク通信の監視
- 多層防御による脅威の軽減

組織内/外のあらゆる脅威に対して、適切な対策を実現します。

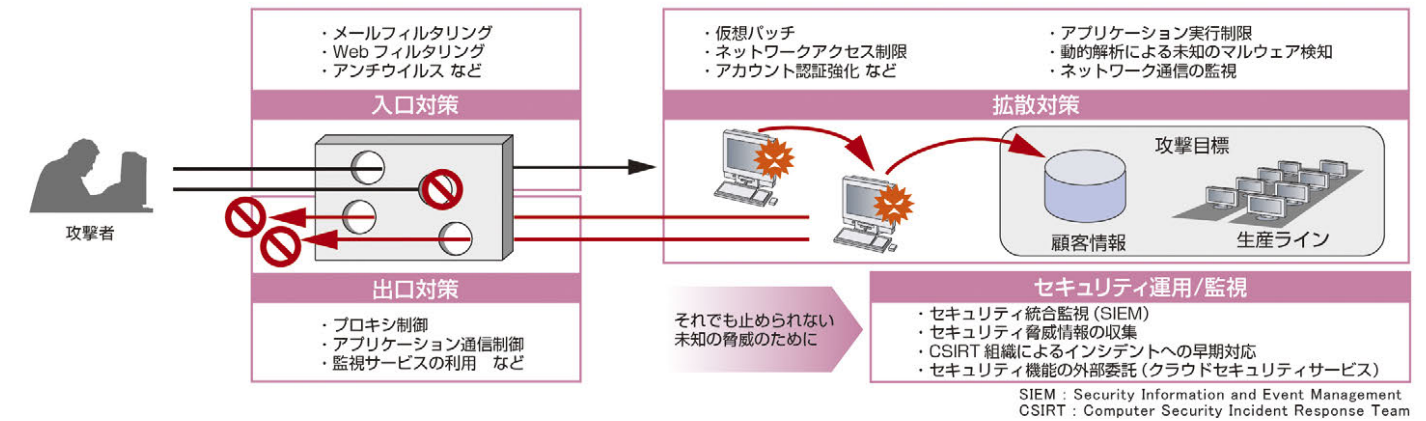
DMZ：DeMilitarized Zone（外部ネットワーク公開エリア） DDoS：Distributed Denial of Service

脅威に対する多層防御でリスクへの対策を実施

脅威＼対策	1 FW	2 IDS/IPS	3 負荷分散	4 VPN	5 無線LANセキュリティ	6 認証	7 マルウェア対策	8 PFW/HIPS	9 WAF	10 メールセキュリティ	11 フィッシング対策	12 URLフィルタリング	13 シンクライアント/暗号化	14 パケットキャプチャ	15 統合ログ管理
❶ マルウェア感染							○	○							○
❷ 不正攻撃 ネット攻撃/Web攻撃	○	○	○				○	○	○						○
❸ 不正アクセス	○	○						○	○					○	○
❹ 盗聴/改ざん				○	○										
❺ なりすまし PC/無線LAN/モバイル					○	○									○
❻ スパムメール/マルウェア付きメール							○			○					
❼ フィッシング									○		○				
❽ 情報漏えい							○	○		○	○	○	○	○	○
❾ 障害															○

ネットワークレイヤの基本的対策　アプリケーションレイヤの対策　ネット経由情報漏えい防止対策　統合管理対策

FW：Firewall　IDS：Intrusion Detection System　IPS：Intrusion Prevention System
VPN：Virtual Private Network　PFW：Personal Firewall　HIPS：Host-based Intrusion Prevention System
WAF：Web Application Firewall

標的型攻撃の手口を踏まえた技術的施策とセキュリティ運用/監視により、インシデントの早期検知を実現し、被害を最小限に抑えます。

SIEM：Security Information and Event Management
CSIRT：Computer Security Incident Response Team

継続した対応が必要なセキュリティ運用を、専門知識を有する技術者によるサービスで提供します。

制御システムへのセキュリティ対策

EWS：Engineering Workstation
HMI：Human Machine Interface

動的解析による標的型攻撃対策